REMARKS

In the February 25, 2005 Office Action, the Examiner rejected claims 1-7, 9-11, 13-19, 21-27, and 29-35 pending in the application. Claims 1-7, 9-11, 13-19, 21-27, 29-31 and 33-35 (3 independent claims; 30 total claims) remain pending in the application. Reconsideration is respectively requested in view of the following remarks.

THE PRESENT INVENTION IS NOT A BACK-UP SYSTEM

The presently claimed invention is not a back-up system. A back-up system creates an archive of files by either copying all files (*i.e.*, baseline back-up) or by copying only those files that have changed (*i.e.*, incremental back-up). Moreover, a back-up system does not include a quarantine area. The presently claimed invention operates in the exact opposite manner of a back-up system. That is, a back-up system preserves changes by "backing up" a copy of any file that has changed. In contrast, the presently claimed invention does not preserve changes; rather, the presently claimed invention **replaces changed files with the unchanged version of the file (*i.e.*, archive copy from the archive file).**

THE PRESENT INVENTION IS NOT AN ANTI-VIRUS SYSTEM

The presently claimed invention is not an anti-virus system. An anti-virus system detects viruses by comparing files to a database of known problems or viruses using rules, but does not compare to archived files. If a virus is detected, the anti-virus system uses rules to repair files or alert a user. Moreover, anti-virus systems do not include an archive file. Since there is no archive, there can be no comparison between a file and an archive copy of that file in an anti-virus system. Also, anti-virus systems limit their detection of files that change to only those files that contain viruses that match their pre-existing list of virus definitions. If a file contains a virus that does not match the pre-existing list of virus definitions, or if a file changes due to means outside of a virus (*e.g.*, automatic updates), the anti-virus system will not consider this file a changed file. Therefore, because the anti-virus system does not recognize these files as changed files, the anti-virus system takes no action on files that change that do not match their pre-existing list of virus definitions. In contrast, the presently claimed invention automatically detects changes to **any** type of file (i.e., to all files, and is not limited to just those files that

contain a virus matching a pre-existing list of virus definitions) by comparing the files to an archive, and if a change is detected, the changed file will be replaced by the archive copy.

CLAIM REJECTIONS FROM OFFICE ACTION

Claims 1, 13, and 21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Korzeniowski, Uncle Sam surfs via Lotus Notes (hereinafter "Korzeniowski") in view of Winn Schwartau, Wipe out Web Graffiti, CNN.com (hereinafter "Winn Schwartau"), and further in view of Chambers, U.S. Patent No. 5,398,196 (hereinafter "Chambers"). Claims 2-7, 9-11, 14-19, 22-27, 29-31, and 33-35 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Korzeniowski, in view of Winn Schwartau, further in view of Chambers, and further in view of Saether et al., U.S. Patent No. 6,405,219 (hereinafter "Saether"). Applicant respectively traverses these rejections.

Korzeniowski generally discloses a brief description of a system for checking and repairing web pages that requires manual intervention to determine if the change was not authorized and, thus, should result in a repair of a web page. While Korzeniowski may detect changes to web pages, Korzeniowski does not disclose or suggest at least the following as similarly recited by independent claims 1, 13, and 21:

- generating an archive
- generating an archive having an archive file
- generating an archive having an archive file, wherein the archive file comprises a master copy of the target file
- detecting changes to the target file by periodically comparing the target file to the archive file
- detecting changes to the target file by periodically comparing the target file to the archive file, wherein the comparison comprises comparing one of the contents, size, and date/time of the target file to the corresponding archive file
- moving the target file from the target location to a quarantine area if the step of comparing indicate that the target file differs from the archive file
- protecting, as necessary, the target file by automatically replacing, without human intervention, the target file such that the target file is identical to the archive file

- protecting, as necessary, the target file by automatically replacing, without human intervention, the target file such that the target file is identical to the archive file, wherein the replacing occurs when the comparison indicates that the target file is not identical to the archive file

On Page 3 of the Office Action, the Examiner asserts that Korzeniowski teaches "generating an archive having an archive file, wherein the archive file comprises a ma[s]ter copy of the target file." Apparently, the Examiner asserts that Korzeniowski teaches this element because the Examiner goes on to state "the archive file needed to be created before the comparison process." Applicant respectively disagrees with this assertion as Korzeniowski simply states that Notes will "notice any change" without disclosing how Notes will carry out this function. Korzeniowski does not provide any details on how Notes will "notice any change." Specifically, Korzeniowski may disclose generally noticing a change, Korzeniowski does not include any comparison between pages or an archive file. As such, Korzeniowski does not mention, teach, or suggest an archive of archive files, or anything that would remotely resemble an archive or archive files. Thus, Korzeniowski certainly does not disclose, teach, or suggest "generating an archive file" as recited by independent claims 1, 13, and 21.

On Pages 3-4 of the Office Action, the Examiner goes on to assert that Korzeniowski teaches the following two claim elements as similarly recited by independent claims 1, 13, and 25: "detecting changes to the target file by periodically comparing the target file to the archive file, wherein the comparison comprises comparing one of the contents, size, and date/time of the target file to the corresponding archive file" and "protecting, as necessary, the target file by automatically replacing, without human intervention, the target file such that the target file is identical to the archive file, wherein the replacing occurs when the comparison indicates that the target file is not identical to the archive file." Applicant respectively disagrees with these assertions.

It appears that the Examiner is relying on one sentence from Korzeniowski for these assertions, as the Examiner quotes the following language from Korzeniowski on Pages 3-4 of the Office Action: "every 4 or 5 minutes, Notes will examine a Web page, notice any change, check to determine if it is legitimate" and "revert to the original format if the change was not authorized." Korzeniowski is limited to formats and web pages, and not, files and changed data within files, as in the presently claimed invention. Even if Korzeniowski may be read as disclosing the detection of changes, this sentence may only be read as teaching that if a change is

detected in a "Web page," then Notes will "revert" the Web page back "to the original format." This does not teach, suggest, or suggest "comparing the target file to the archive file" or "replacing" the "target file such that the target file is identical to the archive file." Korzeniowski does not provide any other details on how Notes operate other than this single sentence. Thus, nowhere does Korzeniowski disclose, teach, or suggest "detecting changes to the target file by periodically comparing the target file to the archive file" or "replacing, without human intervention, the target file such that the target file is identical to the archive file" as similarly recited by independent claims 1, 13, and 21.

Winn Schwartau generally discloses a brief description of Tripwire, a system for checking for unauthorized file modifications. The Tripwire system does not replace any files. The single sentence from Winn Schwartau is as follows: "Systems such as Tripwire can be configured to check for integrity violations – unauthorized file modifications – on a periodic basis (for example, hourly or daily) and will check only those files chosen by the administrator." No further details on the operation of Tripwire are provided by Winn Schwartau. Clearly, this sentence does not disclose, teach, or suggest, *inter alia*, "comparing the target file to the archive file" or "replacing, without human intervention, the target file such that the target file is identical to the archive file" as similarly recited by independent claims 1, 13, and 21.

On Page 4 of the Office Action, the Examiner states "Further more, Chambers discloses in the background of the invention 'the last stand technique of virus detection does not look for anything to do with viruses in particular, but concentrates on the host programs which the viruses attacked.....' (col. 3, lines 17-25). The infected programs (or file examiner interpretation) are detected and isolated by obtaining different values after the check sum process." Chambers generally discloses a process commonly called a "Sandbox." Sandbox technology is the term used to describe the creation of a virtual computer whereby an application is executed inside this controlled environment. While the application is running inside this virtual or special environment, the application can be monitored for malicious behavior. Chambers follows the Sandbox approach by describing a system where any application that is to be executed must first run in this controlled environment. The controlled environment monitors the behavior of the application, and if the application performs any questionable activities, it is determined to be infected with a virus.

In the Background of the Invention, Chambers briefly describes the prior art and discusses why the prior art is not optimal. One prior art method described by Chambers is the

use of a check sum. The check sum item is referred to by the Examiner in the current Office Action (see page 4 of the Office Action). The check sum approach mentioned by Chambers is summarized as an initial run through the computer and calculation of a check sum of all files on the computer. After this check sum is performed and the information is stored, when the end user starts a program, this procedure will compute a new check sum on the current copy of the program file. Then the process compares the new check sum information with the stored check sum information to determine whether the file has been altered. If the current check sum does not match, then the file is considered infected. Chambers mentions that when a file fails the check sum test it can be "isolated." Chambers never reuses the term "isolated" nor does Chambers state the definition of this term.

Chambers teaches isolation to restrict the behavior of a program as it runs to eliminate its ability to infect other programs. That is, Chambers describes the process of isolating the activities of the program of interest from the rest of the computer such that the program cannot infect another program on the computer. This is not relevant to the use of any type of quarantine area. As such, Chambers does not disclose or suggest "moving the target file from the target location to a quarantine area if the step of comparing indicate that the target file differs from the archive file," as similarly recited in independent claims 1, 13, and 21.

In addition, one would not be motivated to combine Chambers with the other cited references. Chambers describes a process of creating a "sandbox" that is a virtual computer system to observe the behavior of a running application. Chambers does not relate to software applications that compare files in order to detect changes to those files. Indeed, Chambers is non-analogous art under M.P.E.P. § 2141.01(a).

> In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the invention was concerned.[1]

Saether generally discloses a system for updating a version of files on a content server. On page 5 of the Office Action, the Examiner states "Saether teaches 'the primary and secondary global servers copy the previous versions of modified source files and restores removed source files from the previous version to at least one sub-directory on the local content servers. This teaches multiple version of the source file." Even if the Examiner's statements regarding Saether

[1] In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992) and see M.P.E.P. § 2141.01(a).

are correct, Saether clearly does not disclose, teach, or suggest, *inter alia*, "detecting changes to the target file by periodically comparing the target file to the archive file" or "replacing, without human intervention, the target file such that the target file is identical to the archive file" as similarly recited by independent claims 1, 13, and 21.

For the above reasons, Applicant submits that the present invention of claims 1-7, 9-11, 13-19, 21-27, 29-31 and 33-35 are patentable over the cited references and therefore claims 1-7, 9-11, 13-19, 21-27, 29-31 and 33-35 are allowable. Accordingly, Applicant respectively request the withdrawal of the rejection of claims 1-7, 9-11, 13-19, 21-27, 29-31 and 33-35 under 35 U.S.C. §103(a).

CONCLUSION

In view of the foregoing, Applicant respectfully submits that all of the pending claims fully comply with 35 U.S.C. § 112 and are allowable over the prior art of record. Reconsideration of the application and allowance of all pending claims is earnestly solicited. If the application is not allowed, Applicant respectfully requests an Advisory Action from the Examiner. Should the Examiner wish to discuss any of the above in greater detail or deem that further amendments should be made to improve the form of the claims, then the Examiner is invited to telephone the undersigned at the Examiner's convenience.

Respectfully submitted,

Date: 25-May-2005

By: David O. Caplan

David O. Caplan
Reg. No. 41,655

Snell & Wilmer L.L.P.
One Arizona Center
400 East Van Buren
Phoenix, Arizona 85004-2202
(602) 382-6284
(602) 382-6070 - Facsimile